

GENERAL RECORDS SCHEDULE 27

Records of the Chief Information Officer

This schedule provides disposal authorization for certain records created and maintained by Federal Chief Information Officers (CIO) and their program offices. This schedule applies to the records of CIOs at agency or departmental headquarters as well as those of deputy and subordinate CIOs at the bureau or field office level. This schedule does not apply to officials with Government-wide responsibilities for information resources management (IRM) and information technology (IT) governance.

In accordance with the Clinger-Cohen Act (originally the Information Technology Management Reform Act), CIOs of 24 major departments and agencies have IRM as their primary duty. They are responsible for advising and assisting the agency's executive with IT acquisition and management; developing and maintaining the agency's IT architecture; promoting the efficient design and operation of the agency's major information resources management processes; monitoring the performance of IT programs of the agency; and developing the knowledge and skill of IT staff. CIOs may also lead, coordinate, or participate in programs to support the mandates of the Paperwork Reduction Act, Government Paperwork Elimination Act, Federal Records Act, E-Government Act of 2002, Privacy Act, Government Performance and Results Act, and other Federal laws and regulations relating to IRM.

This schedule does not cover all records relating to the work of CIOs. CIOs are often responsible for programs and activities whose records are already covered by an approved GRS. Records not described in this or any other GRS must be scheduled by submission to NARA of an SF 115, Request for Records Disposition Authority. If records are part of a larger case file or recordkeeping system that contains records not covered in this schedule, agencies must separately schedule those records or systems by submitting an SF 115 to NARA. If records covered by more than one item in this schedule are maintained together in one file or recordkeeping system, agencies must retain the records for the longest retention period authorized for those items.

The disposition instructions apply to records regardless of physical form or characteristics. Records may be maintained in any format on any medium.

Note that GRS 20, Electronic Records, remains in effect. GRS 20 covers certain temporary files associated with database management. This schedule supplements GRS 20 by providing disposal authority for records relating to the administration of a CIO's office, as opposed to the operation and use of specific systems. This schedule does not apply to the data or information content of IT systems. Records relating to specific systems that support or document the agency's mission must be scheduled individually by submission of an SF 115 to NARA.

1. Information Technology (IT) Program Planning Records

Records relating to the development of agency IT programs. Included are records that document agency-wide IT goals; specify milestones to be achieved; identify performance measures for the agency's IT portfolio; or summarize the underlying principles and approach by which the agency will plan for and manage its IT resources. Records may include strategic and tactical plans documenting the implementation and maintenance of IT systems in support of the agency mission and also may include records supporting formally issued plans, such as records of concurrence, comments, clearances, justifications, and other issuance records.

Cut off annually. Destroy/delete when 7 years old or when no longer needed, whichever is later.

[**Note:** This item does not apply to the data content or design of individual IT systems. Records relating to specific mission-related systems must be scheduled individually by submission of an SF 115 to NARA.]

2. Enterprise Architecture Records

Records identifying the IT systems and networks required to perform the agency's mission and the transitional processes required to implement comprehensive programs to support that mission. Records may include technical reference models, diagrams, graphics, models, and narratives that describe the agency's baseline architecture, target architecture, and related sequencing plans.

Cut off when superseded by a new iteration of the enterprise architecture. Destroy/delete when 7 years old or when no longer needed, whichever is later.

3. IT Capital Investment Records

Records documenting the integration of IT investments with agency-wide strategic planning, budgeting, procurement, and management. Records include routine and periodic reports on IT capital investments; capital asset plans; business cases for major investments, systems, acquisitions, or operational assets identified in the agency's capital investment portfolio; and clearance and review records.

Cut off annually. Destroy/delete when 7 years old or when no longer needed, whichever is later.

[**Note:** Records needed to support contracts are scheduled under GRS 3.]

4. Legal and Regulatory Compliance Records

Records documenting agency compliance with Federal IRM laws and regulations, including systems and reports created to support compliance with the mandates of OMB, GAO, and other Federal IRM and IT oversight agencies.

Cut off annually. Destroy/delete when 5 years old.

5. CIO Committee Records

Records maintained by committees, boards, task forces, conferences, or other IT advisory, governing, or policy bodies for which the CIO has designated sponsorship, leadership, or recordkeeping responsibilities. Records include meeting minutes, summaries, agendas, and transcripts; reports, studies, and publications; membership records; correspondence, mailing, and distribution records; and other administrative committee records.

Cut off annually. Destroy/delete when 5 years old.

[**Note:** Records of Government-wide committees sponsored by CIOs, such as the Federal Chief Information Officers Council, are not covered by this item.]

6. CIO Subject and Office Records

Records not otherwise identified in this GRS that include briefings, reports, presentations, studies, correspondence, and other documents created to support IT program objectives; responses to and decisions on matters affecting the IT program; or operational and managerial guidance to all organizational segments of the agency.

Cut off annually. Destroy/delete when 5 years old.

[**Note:** Official agency policy records generated by the CIO are not covered by this item. They are considered agency policy and issuance records and are scheduled elsewhere.]

7. Schedules of Daily Activities

Calendars, appointment books, schedules, logs, diaries, and other records documenting meetings, appointments, telephone calls, trips, visits, and other activities by the CIO while serving in an official capacity, EXCLUDING materials determined to be personal and those that have been incorporated into other recordkeeping systems.

Cut off annually. Destroy/delete when not less than 2 years but not more than 5 years old.

[**Note:** This item applies only to records of the CIO, not of the office's subordinate staff. See GRS 23/5 for coverage of the latter.]

8. Electronic Mail and Word Processing

Electronic copies of records that are created on electronic and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

- a. Copies that have no further administrative value after the recordkeeping copy is made.

Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

- b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is complete.

**GRS 27, Records of the Chief Information Officer
Implementation Guide**

ITEM TITLE	TYPES OF RECORDS
<p>1. Information Technology (IT) Program Planning Records</p> <p>Cut off annually. Destroy/delete when 7 years old or when no longer needed, whichever is later.</p>	<p>Strategic and tactical plans; reports and statistics documenting quantitative and qualitative performance measures; reports on IT portfolio management; and related clearance and review records.</p> <p>[Note: This item does not apply to the data content or design of individual IT systems. Records relating to specific mission-related systems must be scheduled by submission of an SF 115 to the National Archives.]</p>
<p>2. Enterprise Architecture Records</p> <p>Cut off when superseded by a new iteration of the enterprise architecture. Destroy/delete when 7 years old or when no longer needed, whichever is later.</p>	<p>Technical reference models, diagrams, graphics, models, sequencing plans, and narratives that describe the agency’s baseline or target enterprise architecture (EA).</p> <p>[Note: An “iteration” would typically be the version of the EA (or its component) prepared and submitted to OMB as part of the budget and capital planning cycle. Some agencies may produce and manage EA outside the budget process, which could result in other formal iterations of EA records.]</p> <p>[Note: This item does not cover such records maintained by the Office of Management and Budget as part of its government-wide IRM and IT spending oversight responsibilities.]</p>
<p>3. IT Capital Investment Records</p> <p>Cut off annually. Destroy/delete when 7 years old or when no longer needed, whichever is later.</p>	<p>Reports on IT capital investments; capital asset plans; OMB Exhibit 300 business cases for major investments, systems, acquisitions, or operational assets identified in the agency’s capital investment portfolio; and related clearance and review records.</p> <p>[Note: Contract support records are covered more fully by GRS 3. Offices outside the CIO are likely to maintain similar records to support individual capital investments. GRS 24/9, “Financing of IT Resources and Services,” covers many such records.]</p>

ITEM TITLE	TYPES OF RECORDS
<p>4. Legal and Regulatory Compliance Records</p> <p>Cut off annually. Destroy/delete when 5 years old.</p>	<p>Records of agency-wide compliance with Federal laws and regulations governing information resources management.</p>
<p>5. CIO Committee Records</p> <p>Cut off annually. Destroy/delete when 5 years old.</p>	<p>Meeting minutes, summaries, agendas, and transcripts; reports, studies, and publications; membership records; correspondence, mailing, and distribution records; and other administrative committee records.</p> <p>[Note: Records of Government-wide committees sponsored by CIOs, such as the Federal Chief Information Officers Council, are not covered by this item.]</p>
<p>6. CIO Subject and Office Records</p> <p>Cut off annually. Destroy/delete when 5 years old.</p>	<p>Other mission-related briefings, reports, presentations, studies, and correspondence of the CIO not directly related to the schedule items described above.</p> <p>[Note: Some records related to the compliance of individual IT systems may be maintained with and for as long as the documentation for the system itself. See, for example, GRS 24/5, "Files Related to Maintaining the Security of Systems and Data."]</p>
<p>7. Schedules of Daily Activities</p> <p>Cut off annually. Destroy/delete when not less than 2 years but not more than 5 years old.</p>	<p>Official calendars, appointment books, schedules, logs, and diaries.</p> <p>[Note: This item applies only to records of the CIO, not of the office's subordinate staff. See GRS 23/5 for coverage of the latter.]</p>
<p>8. Electronic Mail and Word Processing</p> <p>See GRS 27.</p>	<p>Electronic copies of records described elsewhere in this schedule.</p>

**Frequently Asked Questions about General Records Schedule 27,
*Records of the Chief Information Officer***

1. To whom does General Records Schedule 27 apply?

GRS 27 provides disposal authorization for certain records created and maintained by Federal Chief Information Officers (CIO). This schedule applies to the records of CIOs at agency or departmental headquarters as well as those of deputy and subordinate CIOs at the bureau or field office level.

2. Does this schedule describe all of the records of Federal CIOs?

Not necessarily. CIOs are often responsible for programs and activities whose records are covered by another General Records Schedule or approved agency records schedule.

3. How does this schedule differ from GRS 20, *Electronic Records*, and GRS 24, *Information Technology (IT) Operations and Management Records*?

GRS 20 and GRS 24 cover certain records associated with the day-to-day operation of individual information systems and related support services. GRS 27 provides disposal authority for records documenting the administration of the office of the CIO and its agency-wide information resources management.

4. How does GRS 27/4, “Legal and Regulatory Compliance Records,” differ from GRS 24/1, “Oversight and Compliance Files”?

GRS 27/4 covers CIO records that document an agency’s compliance with Federal laws and regulations governing information resources management. GRS 24/1 covers records that document an office’s or a system’s compliance with the IT policies, directives, and plans that are typically developed or issued by the agency CIO.

5. Does this schedule cover records related to IT security?

Insofar as they document agency-wide efforts to comply with the laws and regulations that govern IT security, such CIO records would be covered by 27/4, “Legal and Regulatory Compliance Records.” However, records that document the security of individual IT systems – including vulnerability assessments, audits, risk management analyses, and security plans – are covered by GRS 24/5, “Files Related to Maintaining the Security of Systems and Data.” Records related to specific security breaches or incidents are covered by GRS 24/7, “Computer Security Incident Handling, Reporting and Follow-up Records.”

6. Does this schedule cover system data?

This schedule does not apply to the data or information content of IT systems. Records relating to specific systems that support or document the agency’s mission must be scheduled individually by submission of an SF 115 to the National Archives.

7. Do records have to be arranged in these categories?

No. If records covered by more than one item in this schedule are maintained together in one file or recordkeeping system, keep the records for the longest retention period authorized for those items.

8. Is this schedule only for paper records?

No. This schedule applies to records regardless of their physical form or characteristics. Records may be maintained in any format on any medium.